ПОКАЗАТЕЛЬ ФРАКТАЛЬНОСТИ ВРЕМЕННЫХ РЯДОВ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Шостак А.В.[1)], Дорошенко Ю.И. [2)]

[1)] ***Национальный аэрокосмический университет им. Н.Е. Жуковского, ул. Чкалова 17, Харьков, Украина 61070, A.Shostak@csac.khai.edu***

[2)] ***Национальный технический университет "Харьковский политехнический институт", ул. Фрунзе 21, Харьков, Украина 61002, auts@outlook.com***

При выборе наиболее защищенной конфигурации компьютерной системы по уровню информационной безопасности программного обеспечения (ПО) основное внимание уделяется оценке параметров и прогнозированию уязвимостей ПО.

Характеристики уязвимостей ПО получают на основе анализа общедоступных баз данных уязвимостей (БДУ), например, NVD и CVE. На основании данных из этих БДУ для конкретного ПО может быть получен временной ряд $T1$, содержащий временные задержки между соседними уязвимостями, а также временной ряд $T2$, содержащий временные задержки между патчами и соответствующими им уязвимостями.

Оценка показателя Херста H фрактальности временного ряда уязвимостей позволяет судить о самоподобности этого ряда. Значение показателя (коэффициента) Херста H лежит в интервале от 0 до 1.

В случае $0 <= H < 0,5$ говорят о антиперсистентности процесса. Здесь высокие значения процесса появления уязвимостей ПО следуют за низкими, и наоборот. Процесс неустойчив. Другими словами, вероятность того, что на i+1 шаге процесс отклоняется от среднего в противоположном направлении (по отношению к отклонению на i шаге) настолько велика, насколько параметр H близок к 0.

При H=0,5 отклонения процесса появления уязвимостей от среднего являются действительно случайными (абсолютно случайными) и не зависят от предыдущих значений (белый шум), что соответствует случаю броуновского движения.

В случае $0,5 < H <= 1$ говорят о персистентном (поддерживающемся) поведении процесса появления уязвимостей ПО либо о том, что процесс обладает длительной памятью.

Иначе говоря, вероятность того, что процесс на i+1 шаге отклоняется от среднего в том же направлении, что и на i шаге настолько велика, насколько параметр H близок к 1. Т.е. персистентные стохастические процессы обнаруживают четко выраженные тенденции изменения при относительно малом "шуме". Чем H ближе к 1 , тем сильнее тренд (за подъемом наверняка следует подъем, а за спадом – спад).

Именно свойство персистентности оправдывает применение различных авторегрессионных моделей для моделирования и предсказания значений временных рядов уязвимостей, а значит и уровней информационной безопасности ПО. Оценка показателя Херста H выполнена в соответствии с *R/S*-анализом [3].

Посредством вычисления накопленных сумм случайных центрированных значений рассчитывается следующий кумулятивный ряд:

$$X(t,n) = \sum_{i=1}^{t}(X_i - M_x(n)), 1 \le t \le n < N, \quad (1)$$

где X – временной ряд уязвимостей ПО длины N; $M_x(n)$ – среднее арифметическое элементов подпоследовательности ряда X длины n (n – длина скользящего по временному ряду из N чисел окна), $n<N$.

Далее вычисляется функция размаха накопленных сумм $R(n)$ как разность между максимальным и минимальным значениями $X(n)$ для каждой подпоследовательности длины n:

$$R(n) = \max(X(t,n)) - \min(X(t,n)), 1 \le t \le n. \quad (2)$$

Определяется среднеквадратическое отклонение $S(n)$ подпоследовательности длины n:

$$S(n) = \sqrt{S_n^2} = \sqrt{\frac{1}{n-1}\sum_{i=1}^{t}(X(i,n) - M_x(n))^2}. \quad (3)$$

R/S-статистика (нормированный размах накопленных сумм):

$$R/S = R(n)/S(n). \quad (4)$$

Для $p=[N/n]$ ([*] – целая часть *) подпоследовательностей длины n получено усредненное значение нормированных размахов накопленных сумм $RS'(n)$.

Аналогично определены $(x(n), y(n)) = (\ln(n), \ln(RS'(n)))$ – всего k точек (k определяется количеством различных $n - n_{min}=10$, $n_{max}=[N/2]$.

Коэффициент Херста H оценивался на основании метода наименьших квадратов как угловой коэффициент наклона прямой тренда, проходящей максимально близко к полученным k точкам.

Список литературы

1. Белобородов А. Ю., Горбенко А. В., Харченко В. С. Применение аппарата теории массового обслуживания для исследования процессов выявления и устранения уязвимостей программных средств // Радіоелектронні і комп'ютерні системи. 2014. – № 5 (69). – С. 65 – 69.

2. Петров В. В., Платов В. В. Исследование самоподобной структуры телетрафика беспроводной сети // Радиотехнические тетради. 2004. – № 30. – С. 58 – 62.

3. Петерс Э. Фрактальный анализ финансовых рынков: Применение теории хаоса в инвестициях и экономике. – М: Интернет-тренд, 2004. – 304 с.